REMARKS

The Office Action of June 3, 2005 has been reviewed and the Examiner's comments carefully considered. The present Amendment modifies claims 1-12, 14-18, and 20-23, cancels claim 13, and adds new claim 24 in accordance with the originally-filed specification. Support for these amendments can be found, for example, on page 18, lines 5-6 and top of page 22 of the originally-filed specification. No new matter has been added. Claims 1-12 and 14-24 are pending in this application.

Objections to the Specification

In the specification, the Abstract has been amended to address the Examiner's objections and to avoid phraseology such as "disclosed is". In addition, the specification has been amended to overcome the new matter objection. Support for these amendments can be found, for example, on page 19, lines 7-12. Reconsideration of this objection is respectfully requested.

Claim Rejections

Claims 4-6, 8, 10, 11, 16-18, and 21-23 stand rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. Claims 4-6, 8, 10, 11, 16-18, and 21-23 have been amended to more clearly and precisely define the invention. Therefore, withdrawal of the Examiner's indefiniteness rejections of claims 4-6, 8, 10, 11, 16-18, and 21-23 is respectfully requested.

Claims 1, 4-8, 10, 14 and 17-23 stand rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 5,917,913 to Wang in view of U.S. Patent No. 6,092,202 to Veil et al (hereinafter "Veil"). Claims 2, 3, 9, and 15-16 stand rejected under 35 U.S.C. § 103(a) as being obvious over Wang in view of Veil as applied to claim 1, and further in view of Bruce Schneier, Applied Cryptography, 1996, John Wiley & Sons, Second Edition, Pages 43-44 (hereinafter "Schneier"). Finally, claims 11-13 stand rejected under 35 U.S.C. § 103(a) as being obvious over Wang in view of Veil as applied to claim 1, and further in view of U.S. Patent No. 5,742,756 to Dillaway et al (hereinafter "Dillaway").

Independent claim 1 is directed to a digital private key protection device for securely storing a user's digital private key and digitally signing received data. The digital

private key protection device (DPKPD) comprises a digital key storage containing a user's digital private key, a cryptographic engine, a communications port, a user operable input, and a trusted display. The user operable input is connected to the cryptographic engine such that the user can communicate authorization of a trustworthy displayed message. If the user operable input is operated, the cryptographic engine applies the user's digital private key in order to digitally sign the data and then transmits the data externally via the communications port of the digital private key protection device.

Wang, the primary reference in all of the prior art rejections, is directed to a portable electronic authorization device (PEAD) that performs a method for approving transaction requests originating from an electronic transaction system. The method disclosed in Wang includes receiving digital data at the device and using the device to approve the digital data, which generally includes transaction details. The method further includes using a stored and protected PEAD user key to encrypt and sign the received digital data to signify approval of the transaction details.

Veil appears to teach a secure device which utilizes a "trusted display" in connection with a security co-processor. The device seems to contain a private key and the device displays the true results of its operations to the trusted display.

The present invention, as defined in the claims of the present application, is distinguishable from the PEAD device of Wang and the system of Veil. In particular and as specifically set forth in amended independent claim 1, the digital private key protection device of the present invention receives "digital data including a document to be signed from an external device." This distinguishes the present invention from Wang and Veil which teach only receiving transactional data, transactional amounts, or similarly brief transactional fields at their PEAD/systems. The benefit of this full document capability is extremely important in a secure environment where secret documents are being authorized. This full document, in combination with the other claimed features, ensures that data on the trusted display, documents in their entirety, are viewed before authorization. In other words, no signed data leaves the digital private key protection device (DPKPD) of the current invention until it has been viewed and authorized.

This benefit of viewing all documents to be signed is only possible because of the trusted display. In particular and as specifically set forth in independent claim 1, the DPKPD of the present invention includes a trusted display for displaying all data to be

signed. However, both Wang and Veil contemplate displays that are very small. They do not display a document. Therefore, in addition to the DPKPD's novel ability to display the entire document in question, Applicant suggests that the nature of the display further distinguishes the DPKPD over both Wang and Veil.

Wang in column 1, lines 24-32 discusses prior art EFTPOS machines. EFTPOS, or ATM machines as they are commonly known, merely display a dollar amount on the screen, as well as some minor instructions, authentication data, and account choice, and ask the user to approve the amount. There is no requirement or opportunity to display the entire transaction contract or any other document. Wang in column 4, lines 41-44 discloses "[t]he data pertaining to the proposed transaction(s) may then be reviewed by the user, either on a screen **208** of requesting device **202** or optionally on a display screen provided with PEAD". Certainly the screen of the requesting device is not a trusted screen. At Column 4, lines 23-25, Wang notes that transaction data could include details such as transaction ID, the merchant's name, the merchant's ID, the time of the proposed purchase, and the like, making no reference to the entire transaction. There is no teaching or motivation to display a document in its entirety.

Continuing on, Wang in Fig. 6A shows the display reading "TR#4096". Wang in column 6, lines 39-43 describes that a user may view the proposed transaction. Wang in column 10, lines 40-44 suggests that the PEAD would be "a small package that can easily fit inside a purse or wallet". Wang in column 12, line 65 to column 13, line 2 proposes using the PEAD to sign a file. However, Applicant respectfully submits that it is critical to observe that Wang does not propose viewing the file on the display. Indeed, with the display that Wang has proposed, such viewing would be impractical for files of any appropriate size or complexity as of the nature of a document.

Wang in claim 8 claims "displaying said transaction request for viewing by said user on a display screen associated with said PEAD". There is nothing in Wang that could be interpreted as teaching the display of a "document", or of the *complete* detail, including, for example, terms and conditions of any information being signed. In fact, in light of all of the mentioned Wang disclosures, Wang teaches away from displaying all data by teaching a small device for displaying incomplete or pieces of transactional data. It would not have been obvious to take a Wang PEAD and expect to combine that with a trusted display as claimed in the present application.

Applicant respectfully submits that Veil also lacks disclosure of a trusted display for viewing the entire document in a transaction. Veil in column 2, lines 38-42 notes that an untrusted display might result in changed details, "such as transaction values". Veil in column 3, line 1 notes a requirement for "uncompromised acknowledgement and authentication of transactions". Veil in column 7, line 58 to column 8 line 5 discusses the trusted display. It "can be, for example, a small LCD display or alike". "The security co-processor can provide the true transaction amount(s) to the trusted display." Veil in column 8, lines 12-14 notes that the display could be used to facilitate the entry of a PIN. Veil in column 14, claim 9 claims a system including a "trusted display".

Accordingly, there is nothing in Veil's disclosure that can be interpreted as teaching the trusted display of a "document", or of the complete detail of any information being signed. In addition, neither Wang nor Veil, whether used alone or in combination, teaches or suggests a motivation for a digital private key protection device that includes a trusted display as set forth in independent claim 1, as amended. Finally, it also does not follow and is not supported that a "trusted display" be used to display received "documents". As mentioned previously, Wang and Veil both teach the display of "amounts" relating to a financial transaction. An amount is arguably of completely different character to a document. The subject specification provides ample support for what is the nature of a document. Therefore, independent claim 1 is believed to be allowable and reconsideration of the rejections is respectfully requested. Since pending claims 2-12 and 14-24 depend either directly or indirectly from, and add further limitations to, independent claim 1, these claims are believed to be allowable for the reasons discussed hereinabove in connection with independent claim 1.

With regard to claim 4, the present application discloses an audit means for auditing the signing of transmitted signed data. The Examiner has objected to claim 4 citing Wang patet as disclosing an audit means. However, Wang does not reveal any equivalent audit function to that of the present application.

Examiner cites column 7, lines 1-17 as disclosing the audit means of the present invention. This paragraph of Wang describes information that may be sent from the Wang PEAD back to the transaction system, and notes that it can include various information such as user identification and a time stamp. This information is only sent to the transaction system (lines 16-17), and there is no disclosure of the information being sent to any device

for permanent or long-term storage for later review by another authority as is the nature of an audit and understood as such by one skilled in the art. Similarly, in column 12, lines 35-50, Wang has disclosed that approval indication can include certain details that provide useful non-repudiation and integrity properties. However, this does not relate to auditing, i.e., the collection and long-term storage of such information for later review by another authority. Finally, in column 4, lines 40-55, Wang merely indicates that transaction approval information is forwarded back to the transaction system after approval. Again, there is no suggestion of any audit record being kept of such information. Therefore, Applicant respectfully requests reconsideration of the rejection of claim 4.

With regard to claim 5, the present application discloses an audit means for auditing the encryption process of signed data before display. As described previously, the cited passages of Wang do not disclose an audit mechanism. Therefore, reconsideration of the rejection of claim 5 is respectfully requested.

With regard to claim 6, the present application discloses a private key associated to the DPKPD that is used to create an additional signature on the document. The section of Veil the Examiner has cited describes a secure certificate storage memory. As is well know in the art, certificates are digitally signed documents. Digitally signed documents can be verified using a cryptographic engine. But this verification takes time. Veil describes a means of storing pre-verified certificates in a special secure area of memory, so that having been verified once, there is no opportunity for tamper and, hence, no need for a time-consuming re-verification.

While both Veil's system and Wang's PEAD, and a host of other literature, teach the application of the ***user's*** private key for signing transactions, neither patent suggests the use of an additional private key associated with the PEAD/System rather than with the users to create an additional trusted signature. This additional security can be mission critical if used in a security-intensive environment.

A person receiving a signed document has no way of knowing how such a signature was created or, even if it was created using a Veil system or an off-the-shelf PC. In contrast to the Veil system, with the present invention the receiving agent is greatly benefited because not only will the document have a signature of the user, but it will also have a countersignature belonging to the particular device that was used to create the signature. In the current era of rogue software and malicious spy software, this extra signature sets off the

communication from the ordinary run of the mill digitally signed document. It adds an additional layer of protection. So a recipient, should they desire to do so, would be able to verify not only that the user's key was used to create a signature but that this was done using a DPKPD. This would provide that recipient with the assurance that the user had suitable opportunity to review and approve the document in a trustworthy way, and that the user's signature was not created on a less-trustworthy platform such as an off-the-shelf PC. The device signature is analogous to a Justice of the Peace or Public Notary notarization of the user's signature. The present application has additional benefits over the prior art because it provides more assurance to the recipient that the user solemnly and deliberately applied a signature with the intent to be lawfully bound by that signature. In addition, the DPKPD private keys benefit those concerned about security by providing assurance to the recipient that the signature could not have been created by a PC. Therefore, reconsideration of the rejection of claim 6 is respectfully requested.

With regard to claim 7, the present application discloses a DPKPD that can verify the signature generated by another DPKPD. This is something quite different from everything taught by Wang and Veil. Claim 8 further describes a DPKPD according to claim 7 that not only verifies the notary signature but also displays it in a trustworthy way on the trusted display. Again, there is no material in Wang or Veil that would teach this concept or make it obvious to try or create. The concept of having high assurance "notarized" digital signature is novel. While claim 6 describes a DPKPD that can create these notarized (high assurance) digital signatures, claim 7 describes a DPKPD that can verify them. There is nothing in Wang or Veil, as cited by the Examiner, or any other prior art of record that teaches the verification of a signature from another PEAD or Veil system.

With respect to claims 7 and 8, the Examiner points to the information at column 5, line 48 to column 6, line 16 of Veil's patent as a basis upon which to suggest that the subject of claim 1, plus the signature verification defined in claims 7 and 8, are obvious. Veil's description of the well-known characteristics (since 1977, and described by Schneier) of public key (i.e., asymmetric) and symmetric key cryptography describe prior art in which a smart card can be used to store sensitive data, such as a private key.

Wang in column 5, lines 18-22 describes encrypting approval data. In PEAD embodiments where public key cryptography is used, this would require the use of a public key. However, it would be the public key of the system to which the approval data is to be

sent, rather than the public key of the PEAD itself, or the public key of an entity sending data to the PEAD.

Wang in column 7, lines 46-52 describes how a public key of a partner may be used to decrypt a transaction request. If the partner encrypted the information with his own private key, then his own public key would be used for decryption. This would mean that anyone would be able to decrypt the transaction request, which is hardly desirable in this context. Wang in column 8, lines 18-23 contemplates the use of an issuer's public key to "decrypt" configuration information, such as would be used for the installation of a new user's private key. Thus, anyone could check the authenticity and it would not provide any confidentiality. For the purposes of installing a new key, authenticity is required but confidentiality would be desirable too. Wang in column 12, line 65 to column 13, line 2 describes using the PEAD to sign data. But there is no mention of using the PEAD to verify the signature of the data that had been signed by another PEAD. There is no mention in either Wang or Veil that teaches the verification of a notary signature. Therefore, reconsideration of the rejection of claims 7 and 8 are respectfully requested.

With regard to claim 10, the present application discloses decrypting digital data using the user's private key and then displaying the data. The Examiner suggests that Wang in column 7, lines 42-61 teaches claim 10. In the discussion of that section of the Wang patent in regards to claims 7 and 8 above, it was pointed out that Wang has taught the usage of a user's public key to decrypt data. Therefore, reconsideration of the rejection of claim 10 is respectfully requested.

Claims 2, 3, 9, and 15-16 stand rejected under 35 U.S.C. § 103(a) as being obvious over Wang in view of Veil as applied to claim 1, and further in view of Schneier. The Examiner (page 9, para 6.1, line 7) suggests that Veil "further discloses a trusted display for verification of transaction information as discussed above in claim 1." Veil does describe a trusted display on which a user views details of a proposed transaction. However, this is related to the subject of claim 1 and not the subject of claim 2. Rather, claim 2 relates to the trusted display of whether a certain user did or did not digitally sign and authorize a certain transaction. As described previously above (see discussion of claims 7 and 8), there is no aspect of Veil or Wang that describes a process of determining whether signatures applied by the PEAD or Veil's system are now valid or not in a trusted manner.

Veil describes how a public key can be used to verify a digital signature. Veil describes how a security co-processor might authenticate by signing a purchase application, thereby converting it into a purchase response, which is then passed to "any one of the electronic transaction parties". Veil describes how "at the other end, a bank or other transaction partner(s) have their own security mechanism for decrypting the message."

Although the mathematical cryptographic algorithms for verifying the validity of the signature in the response are well known, such algorithms are normally implemented on untrustworthy platforms, such as commodity personal computers with commodity software, that are vulnerable to many threats, as Veil itself identifies. Veil has described a secure environment for creating a signature but it has not proposed or contemplated a secure environment for a recipient to determine whether a signature has been validly created or not. An untrustworthy computer could easily report that a purchase response was validly signed, when that was not the case. There are many e-mail programs with malicious codes that can indicate that a message has been validly signed when it is not the case. It would be useful to have a trustworthy system, as claimed in claim 2 of the present invention, to display whether the signature on a particular signed document is valid or not. Therefore, Applicant respectfully requests reconsideration of claim 2.

Referring to the Examiner's objection to claim 3, 9, and 15-16, these objections may now be overcome in light of amended claim 1. Claim 3 is dependant on claim 1 and claims that the received data includes a digital certificate. Claim 9 has been amended to clarify that the "key storage" includes a plurality of user's public keys. Claim 9 describes a device that can be used to encrypt a message that is to be sent to one of a number of people. Claims 15 and 16 have been amended to clarify the required functionality of the DPKPD's ability to use multiple encryption algorithms and multiple different communication protocols. Therefore, reconsideration of claims 3, 9 and 15-16 is respectfully requested.

Finally, claims 11-13 stand rejected under 35 U.S.C. § 103(a) as being obvious over Wang in view of Veil as applied to claim 1, and further in view of Dillaway. The claims in question have been amended to improve their clarity and, most notably, claim 13 has been canceled. It is to be noted that claims 11 and 12 depend from claim 10, which itself depends from claim 1, and should be allowable since claim 1 is believed to be in condition for allowance.

The Examiner argues first that Dillaway is in an analogous art and discloses the use of a smart card to perform security critical operations, such as user authentication or digital signature generation. Dillaway provides this functionality by arranging communication between an input/output (I/O) controller, on one side of which is a keyboard/PC and the other side of which is the mechanical/electrical smart card interface, and between them is a physically operable Secure Presence Key. When a security critical operation needs to be performed by the smart card, the smart card generates a challenge in the form of a presence enquiry to the I/O controller or a circuit connected between the I/O controller and the reader. It is during the process of the challenge and response or lack thereof that the smart card interface ignores any communications from the I/O controller. This is a blockage of communications *to* the smart card, not a restriction to the communication *from* the smart card itself of any data, as is the subject of claims 10, 11, and 12. In the present application, the DPKPD is restricted from passing data external of the DPKPD and data is only passed to a trusted display.

Furthermore, the smart card of Dillaway is programmed only to perform a security related function if the SPK is (1) actuated and (2) an associated signal received. The smart card is designed to ensure that hostile or careless software cannot utilize critical smart card services without knowledge of the user. This is clearly a different purpose to that of claims 10 to 12, namely, restricting data communication externally. Applicant, therefore, reiterates that subject claims 11 and 12 are novel and non-obvious and respectfully requests reconsideration.

Conclusion

For all the foregoing reasons, Applicant believes that claims 1-12 and 14-23, as amended, are patentable over the cited prior art and in condition for allowance. Reconsideration of the rejections and allowance of all of pending claims 1-12 and 14-24 are respectfully requested.

Respectfully submitted,

THE WEBB LAW FIRM

By _____

Richard L. Byrne
Registration No. 28,498
Attorney for Applicant
700 Koppers Building
436 Seventh Avenue
Pittsburgh, Pennsylvania 15219-1818
Telephone: 412-471-8815
Facsimile: 412-471-4094
E-mail: webblaw@webblaw.com